# SAS Security Documentation Roadmap

Version 1.0  April 12, 2016

**Navigating to the Documentation**

1. Navigate to support.sas.com/documentation and select **Product Index A-Z**.
2. On the **SAS Product Documentation** page, select the letter that corresponds to the first letter of the name of the product or solution.
3. Select the name of the product or solution from the alphabetized list.
4. On the **Documentation** page, locate and select the appropriate document you want to view.

**Base SAS® Procedures Guide**
http://support.sas.com/documentation/onlinedoc/base/index.html
Provides information about the following topics:

- PROC AUTHLIB is a utility procedure that manages metadata-bound libraries.
- PROC HTTP uses HTTPS protocol when certificates of the trusted service are configured. PROC HTTP also supports user identity authentication.
- PROC PWENCODE enables you to encode passwords.
- PROC SOAP uses the HTTPS protocol when certificates of the service to be trusted are configured. This trust store and its password must be provided to the SAS session by setting Java system options.

**DataFlux® Authentication Server: Administrator's Guide and Help**
http://support.sas.com/documentation/onlinedoc/dfauthserver/index.html
Documents authentication as it is done on the former DataFlux® Data Management Platform. Almost all of the clients and servers that used to use the Auth Server now use SAS® Metadata Server for authentication by default. The Auth Server does authentication only. Authorization is handled locally on the servers of SAS® Data Management Platform. This book and help set document how to configure connections to as many as three authentication providers in three separate domains. The server and the doc also describe how user profiles are created and stored on the local host of the Auth Server. The server also provides additional server access controls that are implemented in configuration files. This server is now configured by default to run DataFlux® Secure.

**DataFlux® Data Management Server: Administrator's Guide and Help**
http://support.sas.com/documentation/onlinedoc/dfdmserver/index.html
Describes now the DataFlux Data Management Server maintains local authorization and other local access controls, using groups and IP addresses. The server authenticates by default on SAS® Metadata Server. Legacy installations still use the Auth Server. The DatFlux Data Management Server does not use the authorization features of SAS Metadata Server. DataFlux® Secure is installed by default.

**DataFlux® Secure: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/dfsecure/index.html
This version of SAS/SECURE™ is now delivered by default in a disabled state on all of the former components of the DataFlux Data Management Platform. The software provides Advanced Encryption Standard (AES) encryption, SSL protection for HTTP, and FIPS compliance to meet government regulations.

**Encryption in SAS®**
http://support.sas.com/documentation/onlinedoc/secure/index.html
Provides information about installing, configuring, and using SAS and third-party products to encrypt data. Discusses SAS proprietary, SAS/SECURE™, industry-standard encryption algorithms, and third-party strategies (TLS, SSH) for protecting data and credentials in a networked environment. In SAS® 9.4, SAS/SECURE is included with the Base SAS® software, making strong encryption available in all deployments (except where prohibited by import restrictions).
This document includes SAS system options and environment variables used to configure TLS.

- ENCRYPTFIPS= System Option
- NETENCRYPT= System Option
- NETENCRYPTALGORITHM= System Option
- NETENCRYPTKEYLEN= System Option
- SSLCALISTLOC= System Option
- SSLCERTISS= System Option
- SSLCERTLOC= System Option
- SSLCERTSERIAL= System Option
- SSLCERTSUBJ= System Option
- SSLCLIENTAUTH= System Option
- SSLCRLCHECK= System Option
- SSLCRLLOC= System Option
- SSLPKCS12LOC= System Option
- SSLPKCS12PASS= System Option
- SSLPVTKEYLOC= System Option
- SSLPVTKEYPASS= System Option
- SAS_SSL_MIN_PROTOCOL Environment Variable
- SAS_SSL_CIPHER_LIST Environment Variable
- SSLCACERTDIR Environment Variable
- SSL_CERT_DIR Environment Variable
- SSL_USE_SNI Environment Variable

**SAS/ACCESS® for Relational Databases: Reference**
http://support.sas.com/documentation/onlinedoc/access/index.html
Contains data integrity and security information including sections about DBMS security and SAS security. The individual database information includes options that pertain to security settings.

- Data Integrity and Security
- DBMS-Specific Reference
- LIBNAME Statement Specifics for SAP HANA

**SAS® Anti-Money Laundering: Installation, Configuration, and Administration Guide**
http://supportprod.unx.sas.com/documentation/solutions/aml/index.html
Provides a section on administering security for users and groups. This includes roles, permissions, and capabilities. Also provides information about creating a metadata user account for the post-installation steps.

**SAS® Business Rules Manager: Administration Guide**
http://support.sas.com/documentation/onlinedoc/brm/index.html
Provides a chapter on administering security for groups, roles, and capabilities. Also provides information about configuring your deployment for HTTPS.

**SAS® Companion for UNIX Environments**
http://support.sas.com/documentation/onlinedoc/base/index.html
Includes information about file permissions, functions that have to do with directory and file permissions, and procedure, statement, and system options that have to do with file permissions, assigning passwords to SAS files, and locking files.

**SAS/CONNECT® User's Guide**
http://support.sas.com/documentation/onlinedoc/connect/index.html
Describes how to encrypt data in server and client transfers, how to set up network security, how to start the SAS/CONNECT spawner securely, and how to authenticate the client. Contains all the spawner start-up encryption options. Contains examples of maintaining the SAS server and SAS/CONNECT spawner and how to use encryption.

- Data Security for SAS/CONNECT or SAS/SHARE® Servers
- UNIX: TCP/IP Access Method

**SAS® Customer Due Diligence: Installation, Configuration, and Administration Guide**
http://support.sas.com/documentation/onlinedoc/cdd/index.html - Secure document that is available on a password protected site.
Provides a section on administering security for users and groups. This includes roles, permissions, and capabilities. Also provides information about creating a metadata user account for the post-installation steps.

**SAS® Data Set Options: Reference**
http://support.sas.com/documentation/onlinedoc/base/index.html
Provides comprehensive information about the SAS data set options. Data set options specify actions that apply only to the SAS data set with which they appear. Some data set options provide security for your data sets, such as passwords and encryption. This document includes ENCRYPT= and ENCRYPTIONKEY= SAS data set options, which support AES encryption.

**SAS® Decision Manager: Administration Guide**
http://support.sas.com/documentation/onlinedoc/edm/index.html
Provides a chapter on administering security for groups, roles, and capabilities. Also provides information about configuring your deployment for HTTPS, configuring your deployment for single sign-on authentication, and configuring users that are authenticated through Kerberos.

**SAS® Environment Manager: Administration Module**
Available only through SAS Help interface.
Provides instructions on managing metadata access using SAS Environment Manager.

**SAS® Environment Manager: User Module**
Available only through SAS Help interface.
Provides information about how to administer users, groups, and roles using SAS Environment Manager, in order to track user activity and manage access.

**SAS® Environment Manager: User's Guide**
http://support.sas.com/documentation/onlinedoc/sev/index.html
Provides information about how to administer users and metadata access with SAS Environment Manager.

**SAS® Federation Server: Administration Guide**
http://support.sas.com/documentation/onlinedoc/fedserver/index.html
Provides instructions to configure permissions and privileges for SAS Federation Server and instructions for how to configure data using administration DDL statements.

**SAS® Forecast Server: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/forecast/index.html - Secure document that is available on a password protected site.
Provides information about how to specify security permissions for users and groups. It discusses layers of security broken down into capabilities, metadata permissions, project ownership/sharing, and file system permissions. There is also a section in the pre-installation chapter on using SAS scripts to grant permissions to user groups in UNIX.

**SAS® Forecasting for Desktop: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/forecast/desktop/index.html - Secure document that is available on a password protected site.
Provides information about how to specify security permissions for users and groups. It discusses layers of security broken down into capabilities, metadata permissions, project ownership/sharing, and file system permissions. There is also a section in the pre-installation chapter on using SAS scripts to grant permissions to user groups in UNIX.

**SAS® Guide to Software Updates**
http://support.sas.com/documentation/whatsnew/index.html
Provides information about TLS considerations when upgrading your software.

**SAS® Guide to Metadata-Bound Libraries**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides information about how to set up and administer metadata-bound libraries. Each physical table within a metadata-bound library has information in its header that points to a specific metadata object (a secured table object). The pointer creates a security binding between the physical table and the metadata object. The binding ensures that SAS universally enforces metadata-layer permission requirements for the physical table—regardless of how a user requests access from SAS.

The guide also has several topics related to encryption of the data sets in metadata-bound libraries.

**SAS® Hadoop Configuration Guide for Base SAS® and SAS/ACCESS®**
http://support.sas.com/resources/thirdpartysupport/v94/hadoop/index.html
Discusses Kerberos security requirements for Hadoop.

**SAS® High-Performance Analytics Infrastructure: Installation and Configuration Guide**
http://support.sas.com/documentation/onlinedoc/hpa/index.html
One chapter describes how to deploy the analytics environment with Kerberos.

**SAS® In-Database Products: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/indbtech/index.html
Discusses Kerberos security requirements for deploying the SAS® Embedded Process for Hadoop and SAS® Data Loader for Hadoop.

**SAS® Intelligence Platform: Application Server Administration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides instructions on how to administer the following options and statement, using a SAS Application Server:

- Object Spawner Invocation Options
- LOCKDOWN System Option
- SECPACKAGE System Option
- SECPACKAGELIST System Option
- SSPI System Option
- LOCKDOWN Statement

**SAS® Intelligence Platform: Data Administration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides information about how data set and table-level security are used to create metadata for the tables in a library by registering the tables with SAS® Management Console or with PROC METALIB.

**SAS® Intelligence Platform: Desktop Application Administration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides information about using SAS® Management Console to manage servers, libraries, security, metadata objects, roles, logs, backup and recovery, scheduling, and message queues.

**SAS® Intelligence Platform: Installation and Configuration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides descriptions of SAS® Deployment Wizard configuration prompts and instructions on setting up certificates for SAS deployments. Identifies key reasons why SAS recommends the use of internal accounts. The chapter titled "Setting Up Users, Groups, and Ports" defines the required accounts and privileges. The section titled "Internal User Accounts" contains specific information.

**SAS® Intelligence Platform: Middle-Tier Administration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Documents the security features that are provided by the middle tier. Provides information about the various methods of authenticating the middle-tier components. This includes the following topics:

- Web Authentication
- Support for IBM Tivoli Access Manager WebSEAL
- Support for CA SiteMinder

- Support for Integrated Windows Authentication
- Support for SSL with Client Certificate Authentication
- Apache Authentication
- Using the SAS Anonymous Web User with SAS Authentication
- Configuring SAS Web Server Manually for HTTPS
- Configuring SAS Web Application Server to Use HTTPS
- FIPS 140-2 Compliance

**SAS® Intelligence Platform: Overview**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides a high-level overview of security in the SAS Intelligence Platform.

**SAS® Intelligence Platform: Security Administration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides the security features of the SAS Intelligence Platform. This includes the following topics:

- Essential Information for All Security Administrators
- Authorization
- Authentication
- Encryption
- User Administration
- Checklist for a More Secure Deployment

**SAS® Intelligence Platform: System Administration Guide**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides security information about loggers for metadata server events. Description of security-related properties that can be set in the metadata server configuration file. It also describes options that control the assignment and management of passwords for internal users. This includes the following topics:

- About Metadata Server Loggers
- Reference Information for omaconfig.xml
- Overview of Initial Roles, Groups, and Users
- Who Can Do What: Credential Requirements for SAS Management Console Tasks
- Promoting Access Controls; Promoting Secured Data Folders, Secured Library Objects, and Secured Table Objects; and Promoting Security Objects and Server Objects

**SAS® IT Resource Management: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/itsv/index.html
Information about using the lockdown feature and accessing third-party collectors.

**SAS® IT Resource Management: Report Center Guide**
http://support.sas.com/documentation/onlinedoc/itsv/index.html
Information about permissions, credentials, authorization, authentication, running with secure sockets layer protocol, sign on/off and time-outs.

**SAS® IT Resource Management: Migration Guide**
http://support.sas.com/documentation/onlinedoc/itsv/index.html
Information about encrypting passwords.

**SAS® Language Reference: Concepts**
http://support.sas.com/documentation/onlinedoc/base/index.html
Contains general information about passwords and security in the following chapters:

- SAS Data File Encryption
- Blotting Passwords and Encryption Key Values
- Encrypting Variable Values
- Encryption and Integrity Constraints
- Creating PDF Files Using Universal Printing

**SAS® Libname Engine for SAS® Federation Server: Users Guide**
http://support.sas.com/documentation/onlinedoc/fedserver/index.html
The section titled "SAS Federation Server Security" includes security information.

**SAS® Logging: Configuration and Programming Reference**
http://support.sas.com/documentation/onlinedoc/base/index.html
Provides information about how to generate audit messages for metadata-bound libraries in the section titled "Audit Messages for Metadata-Bound Libraries".

**SAS® Management Console: Guide to Users and Permissions**
http://support.sas.com/documentation/onlinedoc/intellplatform/tabs/admin94.html
Provides instructions on using SAS Management Console to administer users, groups, and roles, set permissions, and work with ACTs. This includes the following topics:

- User Administration Tasks
- Exercises in User Administration
- Access Management Tasks
- Exercises in Access Management

**SAS® Management Console: User Manager Plug-in**
Available only through SAS Help interface.
Provides instructions on how to administer users, groups, and roles using SAS Management Console.

**SAS® Marketing Automation: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/ci/index.html - Secure document that is available on a password protected site.
Provides a chapter on administering security for users and groups. This includes roles, permissions, capabilities, and access control templates.

**SAS® Marketing Optimization Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/ci/index.html - Secure document that is available on a password protected site.
Provides a chapter on administering security for users and groups. This includes roles, permissions, capabilities, and access control templates.

**SAS® Merchandise Planning: Installation and Configuration Guide**
http://support.sas.com/documentation/onlinedoc/merchandiseplan/index.html
The following security topics are documented:

- How to implement HTTPS and SSL security when setting up web server and web application server instances.
- How to use the Security Audit Log feature to capture a record of security-related events for accountability.
- How to set security properties for the application.
- How to control security by authenticating users based on their IDs and passwords, and how to use user groups to provide and restrict user access to certain features and functions.
- How to grant user group access to each interface object (such as a menu item, toolbar button, or option) in the application.

**SAS® Merchandise Allocation: Installation and Configuration Guide**
http://support.sas.com/documentation/onlinedoc/merchandiseplan/index.html
The following security topics are documented:

- How to implement HTTPS and SSL security when setting up web server and web application server instances.
- How to use the Security Audit Log feature to capture a record of security-related events for accountability.
- How to set security properties for the application.
- How to control security by authenticating users based on their IDs and passwords, and how to use user groups to provide and restrict user access to certain features and functions.
- How to grant user group access to each interface object (such as a menu item, toolbar button, or option) in the application.

**SAS® Mobile BI Help**
Available only in the app that is free and publicly available.
Describes security features available in the app and features that affect the security of reports the users might view in the app.

**SAS® Model Manager**
http://support.sas.com/documentation/onlinedoc/modelmgr/index.html
Provides information about web authentication in a topic titled "Configure Your Deployment for Single Sign-On Web Authentication".

**SAS® Real-Time Decision Manager: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/ci/index.html - Secure document that is available on a password protected site.
Provides a chapter on administering security for users and groups. This includes roles, permissions, capabilities, and access control templates.

**SAS® System Options: Reference**
http://support.sas.com/documentation/onlinedoc/base/index.html
Provides reference information about SAS system options, and functions and procedures that operate on system options. Security and authentication options include:

- EMAILHOST= System Option
- PDFSECURITY= System Option
- PDFPASSWORD= System Option
- EMAILAUTHPROTOCOL= System Option
- EMAILPW= System Option

**SAS® MDM: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/mdm/index.html
Provides information about authentication, authorization, auditing, and encryption. Also includes a section titled "Security Consideration for SAS MDM".

**SAS® MDM: User's Guide**
http://support.sas.com/documentation/onlinedoc/mdm/index.html
Provides information about authentication and authorization. Also includes a section titled "Security Consideration for SAS MDM".

**SAS® Social Network Analysis Server: Administration Guide**
http://support.sas.com/documentation/onlinedoc/socialnetworkinfo/index.html - Secure document that is available on a password protected site.
Provides information about using SAS® Management Console to set up and administer the solution. It describes parameters in the Configuration Manager, database tables, and configuration files that control aspects of the user interface.

The section titled "Direct Alert Details Access" provides information about enabling direct access to an alert when a user logs in. The section titled "Configuring External Applications" provides information about how to launch external applications from inside the solution. Examples of stored processes code are included throughout the guide.

**SAS® Social Network Analysis: Installation and Configuration Guide**
http://support.sas.com/documentation/onlinedoc/socialnetworkinfo/index.html - Secure document that is available on a password protected site.
Contains information about creating the SAS Social Network Analysis Server user accounts as well as setting up investigator accounts.

**SAS® Visual Analytics: Administration Guide**
http://support.sas.com/documentation/onlinedoc/va/index.html - Secure document that is available on a password protected site.
Provides a chapter on security information that is specific to SAS Visual Analytics.

**SAS® Visual Process Orchestration Server: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/po/index.html
Includes a chapter titled "Configure Security".

**SAS® Visual Process Orchestration: User's Guide**
http://support.sas.com/documentation/onlinedoc/po/index.html
Contains information about SAS® Metadata Server capabilities and roles for SAS® Visual Process Orchestration.

**SAS® Visual Scenario Designer: Administrator's Guide**
http://support.sas.com/documentation/onlinedoc/vsd/index.html - Secure document that is available on a password protected site.
The "Getting Started" chapter includes instructions about how to use SAS® Management Console to manage servers and add users. It also includes information about host account privilege information for accounts that load data, import data, or start/stop SAS® LASR™ Analytic Server. The "Batch Server Deployment" chapter includes information about how to generate executable *.sas files from a SAS Visual Scenario Designer deployment using a macro. This process connects to the SAS Visual Scenario Designer database to retrieve information. The "Post-installation Considerations" chapter includes information about how to load client-specific data using SAS provided scripts and how to access the PostgreSQL database.